- D R A F T -

STATINTL [redacted] ACCOUNTABILITY FOR AND HANDLING OF CLASSIFIED MATTER

a. Policy

(1) General:

(a) This regulation reflects Agency policy as to the accountability for and handling of classified national security information and material. This policy is based upon and consistent with the requirements of Executive Order 11652 - Classification and Declassification of National Security Information and Material, and of its implementing National Security Council Directive Governing the Classification and Safeguarding of National Security Information.

(b) It is a primary responsibility of all CIA personnel to ensure that classified material is handled in a secure manner and that in no instance unauthorized persons have access to such material. Any employee becoming aware of the loss or possible compromise of classified information shall immediately report this to the Director of Security.

b. Requirement

(1) Accountability Requirements

(a) The Agency is considered a repository storing large volumes of classified material in terms of Executive Order 11652 and its implementing National Security Council Directive; therefore, accountability will be maintained to reflect, the current location, changes in classification, and the final disposition of TOP SECRET material. Finding aids should be maintained for other classified materials.

STATINTL (b) [redacted] Control of AEC Restricted Data, defines Agency policy and procedures relative to the handling of "Restricted Data" in compliance with the Atomic Energy Act of 1954, as amended.

(c) Agency security policy and procedures applicable to the accountability for the handling of sensitive compartmented information as defined in Director Central Intelligence Directives No. 1/14 and 1/16 are described in other regulatory issuances.

(d) Other U.S. Government departments and agencies originate and disseminate particularly sensitive national security information, for which they may establish special accountability requirements. Agency components accepting such material will comply with the controls required by the originator. The Office of Security will provide guidance in handling such requirements as necessary.

(e) The Director of Security is responsible for the management of the Agency's Top Secret Control Program and designates the Agency's control officer's for Treaty Organization (NATO, SEATO, CENTO) and other accountable classified material.

(f) Accountability Records

(1) Centralized Control System: The Director of Security will manage ~~an~~ Agency-wide inventory and control systems for classified accountable matter including TOP SECRET, Treaty Organization, and other accountable material.

(2) Operating officials will be responsible for ensuring that components

within their jurisdictions provide the necessary inputs to this sytem when such material is received from outside the Agency, created within their components, dispatched out-

STATINTL side the Agency to [redacted] Field Stations, destroyed, downgraded, or retired to archival storage.

(3) Local Accountability: Operating officials will maintain appropriate records of local accountability to reflect their local TOP SECRET holdings and in this way complement the centralized control system.

(4) The Director of Security is responsible for conducting periodic physical inventories of TOP SECRET and other classified accountable materials and for investigating the loss of such material.

(2) Handling Requirements

(a) Transmission

(1) Outside CIA:

(a) Classified material destined for outside the Agency may be trans-

mitted only by: approved secure electrical means; Agency employees with staff-like security clearances, who are documented as couriers or are temporarily functioning as couriers with the approval of supervisory personnel; members of Intelligence Community courier services; military courier services; or diplomatic pouch services. In addition,

(b) Within the Continental United States, Secret and Confidential material (not Top Secret) may be transmitted through the U.S. Postal Service using Registered Mail and Return Receipt Requested service;

(c) Restricted Data and sensitive compartmented information may be transmitted outside the Ageny only by authorized couriers, by individuals authorized access to the material which they are delivering, or, by especially authorized electrical channels.

Next 1 Page(s) In Document Exempt

(a) Such material delivered by Agency couriers or staff employees between Agency occupied buildings in the Headquarters area may be enclosed in a single opaque cover marked above as specified in paragraph 25 b (1); and

(b) When delivery is made completely within the controlled environment of an Agency occupied building, such material need only be covered in an appropriate manner to protect it from casual disclosure.

c. Receipting Procedures:

(1) The use of receipts is to assist in ensuring that classified material, when transmitted, reaches its intended recipient. E. O. 11652 requires the attachment of a document receipt within the inner cover of transmitted Top Secret and Secret material and its return by the recipient to the sender.

(a) Receipt Form ( ) will be used for this purpose when such material is transmitted outside the Agency.

?

(b) For the transmittal of such material within the Agency document receipts will be used where required by accountable classified material control procedures.

(2) Courier receipts will be used as necessary to control the point to point transmission of classified material.

(3) Destruction of Classified Material

(a) The destruction of classified material must be accomplished in accordance with existing law and regulation. Custodians of Documents will survey periodically material in their possession and, if deemed of no further use, will request their Area Records Officer to review the documents and give directions for appropriate disposition as provided in Agency regulations.

STATINTL

[redacted]

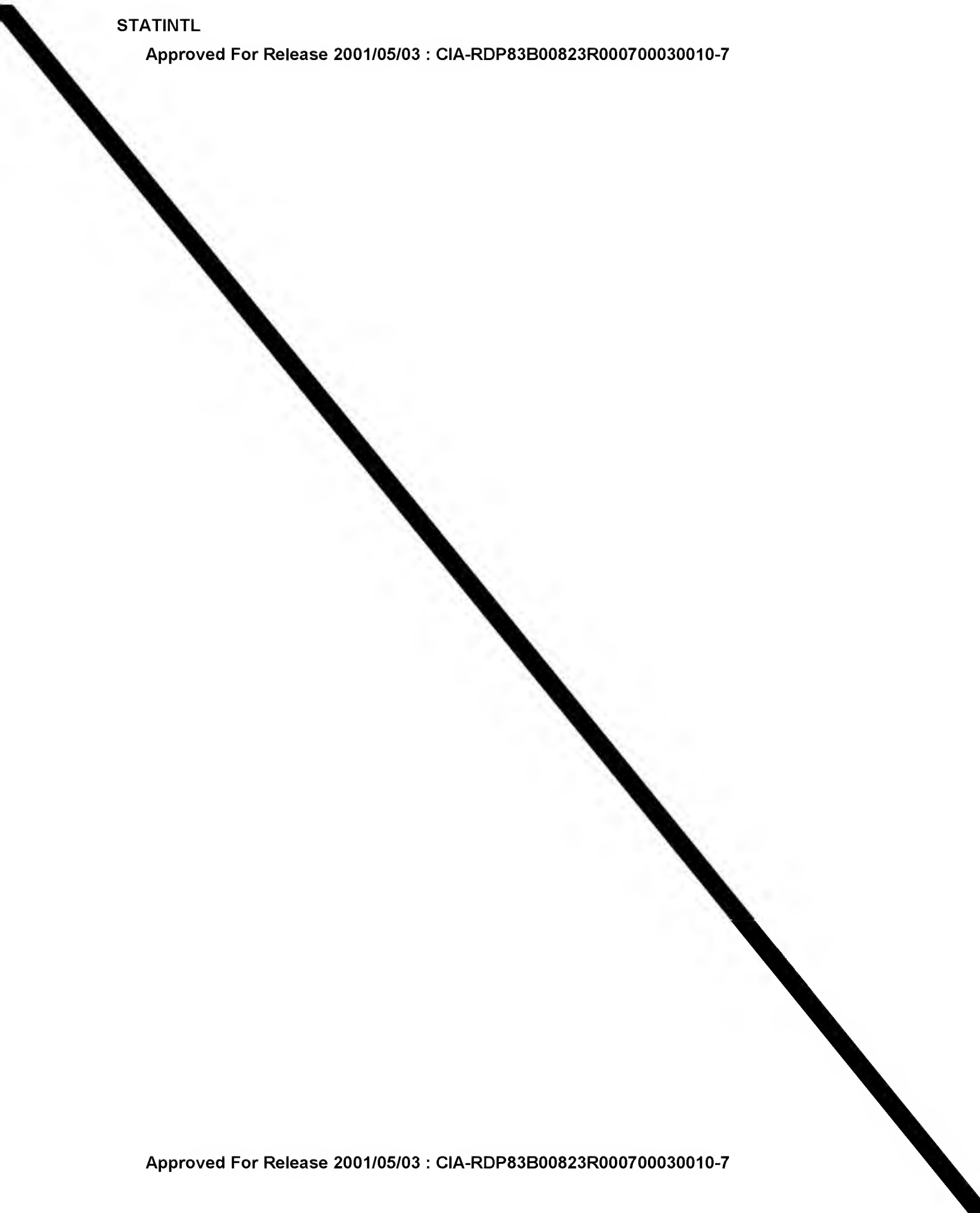
[redacted] STATINTL

3. CLEARANCE OF PERSONNEL FOR DUTY WITH CIA. This paragraph prescribes the security criteria and investigative requirements governing the security clearances of the following categories of Agency personnel: staff employees, staff agents, military and civilian personnel detailed or assigned to CIA and placed in staff positions, consultants, and contract employees who are to have staff-like access to Agency installations or information. The same security criteria and investigative requirements apply to contractor personnel operating on behalf of the Agency at the TOP SECRET level.

a. AUTHORITY. The authority for the criteria and procedures prescribed herein is contained in the Act of August 26, 1950, 64 Stat. 476; Section 102 of the National Security Act of 1947; the Central Intelligence Agency Act of 1949, as amended; and Executive Orders No. 10450 of April 27, 1953, as amended, No. 10491 of October 13, 1953, as amended, and No. 10501 of November 5, 1953, as amended.

b. POLICY

STATINTL [redacted]



Approved For Release 2001/05/03 : CIA-RDP83B00823R000700030010-7

STATINTL

[redacted]

(3) FINAL SECURITY DECISION AS TO ACCEPTABILITY. Reports of investigations and all other available information on an individual will be reviewed and appraised by officials so designated to perform this function. In each case a recommendation for acceptance or rejection will be made to the Director of Security, who will make final security decision as to the acceptability of the individual for assignment to or retention in CIA, except those cases which, in his opinion, or in the opinion of an interested operating official, should be referred to the Director of Central Intelligence for final decision.

(4) PROVISIONAL CLEARANCE

(a) Individuals who enter on duty with the Agency in a provisionally cleared status have rigid conditions attached to their employment while in such a status which preclude the full utilization of their qualifications and experience. Provisionally cleared employees will not:

(1) Have access to classified material or secure areas;
(2) Be issued a badge or credential;
(3) Be assigned to any unclassified duties other than those listed in the clearance.

(b) As a matter of Agency policy, individuals will not be employed on the basis of a provisional clearance unless their service would otherwise be lost to the Agency.

(1) A provisional clearance may be granted to clerical personnel possessing typing, stenographic, or other clerical skills, and to extremely well-qualified individuals whose professional skills and knowledges are needed by the Agency. Since individuals employed in professional or technical positions usually have established relationships in their occupational field and often have personal

or financial commitments, their failure to meet Agency standards for full-duty status ordinarily imposes greater hardship upon them than is true in the case of clerical employees. The probability of individual embarrassment and hardship and adverse ability of individual embarrassment and hardship and adverse criticism of the Agency is so great in such cases, that employment of professional personnel under provisional clearance should not be considered except in unusual cases.

(2) Persons gainfully employed at the time security processing is initiated should not be considered for entrance on duty under a provisional clearance unless such employment is not expected to last during the processing period.

(c) Under no circumstances should provisionally cleared employees move their families or household goods to the area of their CIA employment. The supervisors responsible for the administrative control of such individuals will impress upon them the temporary nature of their appointments and will advise them against making any substantial change in their personal affairs or financial arrangements prior to receiving full clearance.

(d) A request for the provisional clearance of an applicant for a position in grade GS-7 or above will require the approval of the Deputy Director concerned. If it is considered necessary to request the appointment of an individual on a provisional clearance at grade GS-7 or above, the requesting office will attach a justification of the proposed action, approved by the appropriate Deputy Director, to the Standard Form 1152, Request for Personnel Action, requesting the individual's appointment.

(e) During the period of provisional employment, the office which requested appointment of a provisionally cleared employee in grade GS-7 or above will be responsible for providing a work assignment under proper supervision, in accordance with the provisions outlined in subparagraph (4) (a) above. Personnel on provisional clearance in grade GS-6 or below will normally be assigned to unclassified work projects under supervision of the Office of Personnel while awaiting full clearance. Under exceptional circumstances, the requesting office may arrange with the Office of Personnel to assume responsibility for providing unclassified work assignments to provisionally cleared employees in GS-6 or below; however, the Office of Personnel will retain administrative supervision of such personnel.

(5) USIB NOMINATIONS. Individuals nominated by USIB agencies for duty with CIA will be accepted only under conditions prescribed in subparagraphs c(2) and (3) above. Each nomination should contain statements to the effect that the individual nominated:

(a) Has (or has not) had a minimum of 10 years prior honorable Government service.

(b) Is (or is not) cleared for access to TOP SECRET matter in the nominating agency, and the basis for clearance.

(c) Is considered by the nominating agency, based on such information and records as are available in that agency, to possess qualities of integrity and loyalty sufficient to warrant assignment to duties involving matters of concern to the national security.

(6) CONSULTANTS. Clearance of consultants will be governed by the following instructions:

(a) Preliminary clearance will be obtained from the Director of Security before contacting any individual to determine willingness to serve CIA as a consultant.

(b) After determination of willingness has been obtained:

(1) Full security investigation will be made in each case.

(2) Clearances shall bear stated restrictions, if security investigation indicates that full clearance cannot be granted and sufficient justification for restricted employment can be presented by the CIA activity concerned. Such justification will include the circumstances under which the consultant will be used and the classification of the information to be divulged. The approval of the Director of Central Intelligence will be required for each restricted clearance.

d. EXCEPTIONS AND APPEALS

(1) EXCEPTIONS. Exceptions to the provisions of subparagraphs b(1)(b) and b(1)(d) will be granted by the Director of Security only upon receipt of written justification from an Operating Official, and will be subject to such limitations on duties and assignments as are deemed necessary in the interests of the Agency by the Director of Security. Exceptions to subparagraph b(1)(b) may be granted when the Office of Security is able to conduct a valid background investigation of the applicant and provided there are no other disqualifying factors. Exceptions to the provisions of subparagraph b(1)(c) may be granted by the Deputy Director for Administration upon receipt of written justification from an Operating Official, concurred in by the cognizant Deputy Director and the Director of Security. Exceptions to any other provisions of this paragraph may be granted only by the Director of Central Intelligence.

(2) APPEALS FROM SECURITY DISAPPROVAL. In those case of security disapproval of clearances when the need for the services of the individual is considered so great that Agency operations may suffer if he cannot be used, the following procedures shall apply:

(a) The Operating Official concerned shall notify the Director of Personnel of his objection to the disapproval, and his reasons therefor, and the Director of Personnel shall so advise the Director of Security.

(b) The Director of Security and the Operating Official concerned shall discuss the security implications of the disapproval.

(c) If the Operating Official desires to appeal the disapproval, he shall advise the Director of Personnel, through the Deputy Director concerned.

(d) In the case of a consultant, the Director of Personnel will arrange to meet with the Director of Central Intelligence, the Operating Official or Deputy Director concerned, and the Director of Security to discuss the unusual need for use of the consultant, and the security aspects of the case. The Director of Central Intelligence makes the final decision.

(e) In the case of an applicant other than a consultant, the Director of Personnel will forward the appeal to the Director of Security, who will refer the matter, with supporting information, to the Director of Central Intelligence for final decision.

e. REINVESTIGATIONS. The Director of Security will ensure a continuous review of employee files. Normally, this review should be made when there is a pending change of status of the employee but in every case on a cycle of at least five years, and will be followed by an appropriate reinvestigation Reinvestigation will be tailored to meet the cover, operational, and administrative considerations affecting the employee and the Agency.

f. CLEARANCE OF INDUSTRIAL CONTRACTOR PERSONNEL UTILIZED ON CIA FUNDED CONTRACTS. This paragraph prescribes the security criteria and investigative requirements governing the security approvals of industrial contractor personnel utilized on CIA funded contracts.

(1) Authority. The authority for the criteria and procedures prescribed herein is contained in Section 102 of the National Security Act of 1947; the Central Intelligence Agency Act of 1949, as amended; and Executive Orders No. 10450 of April 27, 1953, as amended, No. 10491 of October 13, 1953, as amended and No. 11652 of March 8, 1972.

(2) Policy. A contractor's employee may receive a Security Approval to perform his duties as follows:

(a) At the place of business of the contractor

(b) In an Agency Headquarters environment

If a contractor's employee is approved to perform in one of the two categories above and it is later desired to utilize him in another category his use is considered to have been substantially changed and it will be necessary to submit a new request for a Security Approval to the Office of Security

(3) Responsibilities. The Director of Security is responsible for granting security approvals for the utilization of contractor's employees.

(4) Definitions. Four types of security approvals are utilized in the Industrial Security Program. These are:

(a) Industrial Security Contact Approval (ISCA) This approval is required to permit contact with a prospective CIA industrial contractor's employee to engage in pre-contract discussions.

(b) Industrial Security Approval - Secret (ISS) This approval is required to allow a contractor's employee to work on an Agency funded contract at the Secret level, without access to an Agency installation.

(c) Industrial Security Approval - Top Secret (IST) This approval is required to allow a contractor's employee to work on an Agency funded contract at the Top Secret level without continuing access to an Agency installation.

(d) Industrial Security Staff Approval (ISSA) This approval is required to allow a contractor's employee to work on an Agency funded contract at the Top Secret level with continuing access to an Agency installation.

(5) Procedures. To ensure that industrial contractor personnel being utilized on Agency funded contracts meet appropriate security standards, the following procedures will be applied in the investigation and security approval of such individuals.

(a) Minimum Investigation. The minimum investigation for the various types of Industrial Approvals will consist of the following:

1. Industrial Security Contact Approval (ISCA) An ISCA up to the Secret level may be granted after the Office of Security has verified that the individual holds a defense clearance at the Secret level with another government agency. An ISCA at the Top Secret level may be granted only upon the completion of a 15 year background investigation.

2. Industrial Security Approval - Secret (ISS) An ISS may be granted after appropriate National Agency Checks have been conducted by the Office of Security.

3. Industrial Security Approval - Top Secret (IST) An IST may be granted after appropriate background investigation and National Agency Checks have been conducted by the Office of Security.

STATINTL The minimum investigation will comprise coverage as set forth in [redacted] as well as such other inquiries as the Director of Security may deem appropriate in order to ensure that the contractor's employee meets staff standards for continuing access to Agency installations.

(b) Security Disapproval. A contractor's employee may be security disapproved for access to an Agency funded contract upon a determination by the Director

STATINTL of Security that such access would represent a security risk to the Agency.

g. [redacted]

Next 2 Page(s) In Document Exempt

D R A F T
23 May 1975

STATINTL [redacted] SECURITY

19. COMPUTER SECURITY POLICY AND RESPONSIBILITIES

a. GENERAL

The maintenance of high security standards relating to computer operations or associated information handling techniques is critical for the protection of official data. This is due in part to the storage and availability of large quantities of information residing within a system or location. In addition, the ease of retrieval or manipulation of the information creates unusual security hazards. Thus, security precautions must be considered and analyzed from the outset in the design of any computer system and in the procurement of new computer equipment. System configuration will be dependent upon a number of related factors, but they will include the security policy listed in [redacted] as a minimum.

STATINTL

b. POLICY

(1) PHYSICAL ACCESS CONTROL

(a) A Computer Center

(1) There will be a limited entrance to a computer center. When a center is not in operation, it must be secured in accordance with the requirements of the data stored and processed therein. All doors other than employee access must be locked and used only in event of emergencies or to move equipment and supplies.

(2) Controls will be established to limit access into the machine area of the computer center to authorized personnel. Furthermore, all computer equipment must be behind a control point established to limit access.

(3) If a computer center does not operate twenty-four hours a day, records will be maintained of any use of the equipment during off-shift hours.

(b) Portable Storage Media

Accountability logs must be maintained on portable storage media at all times. All tapes and portable disk packs will be maintained in a controlled area whenever they are not mounted on a system.

(c) Remote Job Entry Stations and Data Access Centers

A room containing a cluster of terminals and/or a remote job entry capability for batch processing must be monitored during hours of operation to ensure only authorized personnel are provided access to the equipment.

(d) Terminals

(1) A terminal will be monitored whenever it is connected to the system. There will be control of access to a remote terminal of a computer system by at least two employees who will ensure that only authorized personnel use the terminal.

(2) Controls will be established to ensure proper terminal connection and to ensure proper operating conditions.

(2) PROTECTION OF INFORMATION WITHIN A COMPUTER SYSTEM

(a) Procedural and Physical Security

(1) All portable storage media will be marked with a classification label which will correspond to the highest classification of data stored therein. Any access restrictions placed upon the data will be contained on the label as appropriate.

(2) Unescorted personnel with direct access to a computer center will have at least a TOP SECRET Agency staff-type clearance and an administrative access approval for all data stored or processed by the system. Any user allowed access to a computer terminal must possess a staff-type TOP SECRET security clearance and an access approval for Special Intelligence information as a minimum.

Special access approvals will be required for all compartmented data designated for input/output at that terminal.

(3) A computer center will be secured in a manner commensurate with the highest classification of the information contained therein. Remote terminals will be secured in a manner commensurate with the data designated for input/output at that site, but in no case less than Agency TOP SECRET/Special Intelligence.

(b) Hardware and Software Controls

All computer systems shall contain the following hardware/software features as an absolute minimum. Measures shall be implemented to provide special controls over access to and/or modification of these features.

(1) Security Labels: Security classification and other required access control labels shall be identified with the information and programs in the system to ensure proper security control of data while in the system and appropriate labeling of output.

(2) User and Terminal Identification/ Authentication: System operation shall include a mechanism that identifies and authenticates personnel and terminals accessing it. This mechanism shall consist of software and/or hardware devices, manual control procedures at terminal sites, and other appropriate measures designed to validate the identity and access authority of system users and terminals.

(3) Memory Protection: Hardware and software control shall be exercised by the system over the addresses to which a user program has access.

(4) Separation of User/Executive Modes of Operation: The user and executive modes of system operation shall be separated so that a program operating in user mode is prevented from performing unauthorized executive functions. Controls shall be implemented to maintain continued separation of these modes.

(5) Residue Clean Out: Measures shall be implemented to ensure that memory residue from terminated user programs is made inaccessible to unauthorized users.

(6) Access Control: Effective controls shall be implemented to limit user and terminal access to authorized information and programs as well as to control read and/or write capability.

(7) Audit Trail Capability: Each system shall produce in a secure manner, an audit trail containing sufficient information to permit a regular security review of system activity by the Office of Security.

(c) Backup Files and Processing

A contingency plan for operations during and/or after an emergency should be prepared by responsible officials of a computer system. Operating officials should identify critical data in a computer system and consider the need to maintain this data in a backup file in the event that the main computer facilities are damaged or destroyed. Backup processing facilities should be addressed in any contingency plan.

(3) Control and Disposition of Magnetic Storage Media

Magnetic storage media shall be safeguarded in the manner prescribed for the highest classification and for all types of compartmented information recorded thereon until destruction of the media or until execution of approved sanitization procedures. The approved sanitization procedures are contained in the paper titled Intelligence Community Policy for the Release of Magnetic Storage Media which was effective 13 March 1974. Sanitization procedures

shall be effected by the operating component and approved by the Office of Security prior to release of the storage media.

(4) Communication Links

All circuitry over which classified data is communicated in plain text form within the Headquarters Building must be installed in accordance with security standards for the Headquarters Plain Text Data Distribution System. Classified data communicated out of any Agency building via a computer communication system must be encrypted. Communication links for computer systems in other Agency buildings will be in accordance with the requirements contained in the Security Standards for Plain Text Data Distribution Systems in Outside Buildings.

(5) Safety

Safety considerations for a computer center and related equipment will be in accordance with the Williams-Steiger Occupational Safety and Health Act of 1970. The CIA Safety Officer must be consulted during construction and alteration of a computer center or any room containing a cluster of terminals or peripheral computer equipment.

c. RESPONSIBILITIES

(1) DIRECTOR OF SECURITY. The Director of Security is responsible for:

(a) developing and publishing security policy and standards for maintaining the security of Agency computer and/or related information handling systems;

(b) coordinating an Agency program for identifying and resolving security problems associated with the use of computers in the processing of official data;

(c) providing guidance to Agency components and users in the handling of computer security problems;

(d) conducting security inspections, surveys, and analyses of Agency and contractor computer systems to evaluate and ensure implementation of computer security standards and policy;

(e) providing Agency support to computer security efforts of the Intelligence Community;

(f) providing Agency support to computer security efforts of certain foreign intelligence and security services as directed.

(2) DIRECTOR OF COMMUNICATIONS. The Director of Communications is responsible for the technical aspects of Emanations Security (EMSEC) as it pertains to the computer processing of official data.

(3) OPERATING OFFICIALS. Operating Officials maintaining computers are responsible for:

(a) implementing Agency security policy and standards for computers within their areas of cognizance;

(b) instituting appropriate procedures to facilitate the security classification of computer output material from computers within their areas of cognizance.

(4) PERSONNEL SUBJECT TO THIS PARAGRAPH. Agency personnel using computer services are responsible for:

(a) adhering to security policy, standards, and procedures defined by the Office of Security and implemented by the Operating Officials maintaining the computer;

(b) ensuring that all forms of computer output material is properly classified and marked in accordance with the provisions of

STATINTL [redacted]

(c) making sure that computer output material which contains job control language and/or a volume table of contents be handled as controlled material;

(d) ensuring that all computer output material is disposed of in the same manner as classified waste.

(5) Insofar as the above responsibilities affect field installations of the Operations Directorate and of the Directorate of Science and Technology, their implementation will be coordinated with the Deputy Director for Operations and the Deputy Director for Science and Technology, respectively.